candidate within the tenderable range of the contract, and attempting to decode each of said plurality of bids using said next closest decode parameter,

wherein said plurality of bids are attempted to be decoded using successive decode parameters corresponding to successive contract price candidates until at least one bid is successfully decoded.

REMARKS

The 25 June 2002 official action addressed claims 1-8. Claims 1-8 are amended and new claims 9 and 10 are added. Claims 1-10 are pending.

Substitute specification

The undersigned has prepared a substitute specification to editorially amend the application to use more typical phrasing and grammar. The undersigned has been careful to only restate what was supported in the original application. No new matter is added.

In the event that the examiner feels that new matter has been added, the undersigned would appreciate an indication of the text that is believed to constitute new matter so that corrections can be focused directly on those portions.

Claim amendments

The claims have been amended in a manner similar to the specification to more clearly express their subject matter.

The amendments are also intended to clarify the feature that different encode and decode parameters are associated with each possible bid within a range of bids, such that each bid is encoded and decoded using corresponding code and decode parameters, and bids are examined by attempting to apply the decode parameters for the possible bids within the range sequentially. This feature is fully supported in the original specification.

The claims are also amended to eliminate the term "means" to clarify that the claims are not intended to be subject to the interpretive provisions of 35 USC §112(6).

In addition, new independent claims 9 and 10 are added. Claim 9 recites a method performed in a bidder's system for encoding and transmitting a bid, and claim 10 recites a method performed in a bid receiver's system for decoding received bids. The features recited in these claims are analogous to those already recited in claim 1, and so it is believed that no new issues are presented and that the new claims should not be subject to restriction.

No new matter is added.

Claim objections

The objected portions of the claims have been corrected by amendment.

Rejections under Section 112

The portions of the claims rejected under section 112 have been corrected by amendment.

Prior art rejections

Claims 1-8 were rejected under 35 USC §103(a) as being obvious over Togher (U.S. 5,375,055). It is believed that the patentable distinctions of the claimed invention over Togher will be apparent from the following discussion.

The claimed invention pertains to a system for submitting and decoding bids, such as in an auction or a lowest-bidder contract award system. In accordance with the claimed invention, each bid within a range of possible bid values (the "tenderable range") has a corresponding code parameter that is used to encode only bids having that bid value. Thus bidders code their bids using the code parameter that corresponds to their particular bid, and send messages that include the coded bids to a bid receiver.

The bid receiver possesses the decode parameters for each possible bid ("contract price candidate") in the tenderable range, and determines the winning bid by applying the successive decode parameters to the received bids, starting

with the highest or lowest (depending on the type of system), until at least one of the bids is decoded. This allows the system to determine the winning bid(s) without revealing any of the other bids, since only the winning bid(s) are decoded, and other bids are not decoded and thus remain confidential. Further benefits of this scheme such as bidder anonymity are discussed in the application.

Togher discloses a system for trading currencies, and Togher's system does include consideration of bid values. However, Togher does not disclose or suggest the particular system in which individual code parameters are associated with each possible bid, and decoding is performed as described above. It is believed that the most relevant portion of Togher is found at col. 14, line 40 - col. 15, line 22, where Togher's bid acceptance process is discussed in detail. It seen from this section that Togher is concerned with determining whether a bidder for a currency transaction has enough credit with the party receiving the bid to engage in the proposed transaction. To that end, Togher loops through all quotes (bids) in an ordered quote list, and for each quote, it is determined whether there is sufficient credit between the parties and a sufficient quoted amount at issue to enable the quote to be accepted (col. 14, line 62 - col. 15, line 17). Thus while Togher does engage in a sequential processing of bids, this processing clearly does not involve processing using code and decode parameters associated with each bid value, as is provided in the claimed invention. Therefore it is believed that the present claims are patentably distinguished from Togher.

The foregoing amendments and remarks address all bases for rejection and are believed to place the case in condition for allowance. The examiner is invited to contact the undersigned to resolve any remaining issues.

Respectfully submitted,

Date: September 25, 2002

for Ronald Coslick Reg. No. 51,991
Registration No. 36,489

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kazue SAKO

Title: ELECTRONIC TENDER SYSTEM

Appl. No.: 09/472,900

Filing Date: 28 December 1999

Examiner: B. GEHMAN

Art Unit: 3629

VERSION SHOWING CHANGES MADE IN REPLY TO 25 JUNE 2002 OFFICIAL ACTION UNDER 37 CFR§1.111

Commissioner for Patents
Box NON-FEE AMENDMENT
Washington, D.C. 20231

Sir:

In reply to the 25 June 2002 official action, the application is amended as follows:

In the specification:

A substitute specification and a marked up version showing changes made to the original specification are submitted herewith.

In the claims:

1. (Amended) An electronic tender system for accepting as a contract price the highest or lowest price among ~~bidding price~~bids ~~offered by a plurality of tenders~~, comprising:

a bidder sub-system including:

a code parameter acquisition ~~means~~ section for ~~taking as input~~receiving a ~~bidding price~~bid selected by the ~~tender bidding~~bidder sub-system within ~~the~~ a tenderable range, and for acquiring a code parameter ~~depending on~~corresponding to the ~~bidding price~~bid,

a code processing ~~means~~ section for using the code parameter obtained by said code parameter acquisition ~~means~~ section to encode said bid, and

a transmission ~~means~~ section for sending a ~~coded~~ message including an encoded bid encoded by said coding ~~means~~ section to a tender opening sub-system, and

a tender opening sub-system including:

a reception ~~means~~ section for ~~accepting said~~ receiving messages from bidder sub-systems including encoded ~~bidding price~~bids until ~~the~~ a closing ~~day~~ time,

a candidate price selection ~~means~~ section for ~~selecting~~ sequentially selecting ~~a~~ contract price candidates ~~from the~~ beginning with one of a highest ~~or~~ and ~~the~~ a lowest ~~among acceptable bidding prices~~within said tenderable range,

a decode parameter acquisition ~~means~~ section for acquiring a decode parameter corresponding to ~~the~~ a contract price candidate selected by ~~said~~ the selection ~~means~~ section, and

a ~~retrieve means~~ determination section for ~~retrieving~~ decoding encoded bids using a decode parameter corresponding to a contract price candidate selected by the selection section to determine ~~if~~ whether a ~~same bidding price~~bid that is the same as ~~the~~ the contract price candidate selected by ~~said~~ the selection ~~means~~ section exists among encoded ~~bidding price~~bids ~~accepted~~ received by ~~said~~ the reception section~~means using said decode parameter~~.

2. (Amended) The electronic tender system as claimed in claim 1, wherein the code processing ~~means~~ section of ~~said~~ the bidder sub-system~~,~~ encodes a ~~fixed~~ bid value using the code parameter obtained by ~~said~~ the code parameter acquisition ~~means~~ section, and

wherein the retrieve ~~means~~ section of ~~said~~ the tender opening sub-system includes a decoding ~~means~~ section for sequentially decoding encoded ~~bidding price~~bids received by ~~said~~ the reception ~~means~~ section ~~according to~~using the decode parameter acquired by ~~said~~ the decode parameter acquisition ~~means~~section, and a ~~judgement~~judgment ~~means~~ section for judging that ~~the~~ a coded ~~bidding price~~bid is identical to ~~the~~ a contact price candidate selected by ~~said~~ the selection ~~means~~ section ~~in the case where~~ when the decoding result ~~becomes~~ is equal to said fixed value.

3. (Amended) The electronic tender system as claimed in claim 1, wherein the code processing ~~means~~ section of ~~said~~ the bidder sub-system~~,~~ ~~includes a~~ performs encoding ~~operation of the fixed price by~~ using a public key corresponding to ~~said~~the ~~bidding price~~bid, and

wherein the decoding ~~means~~ section of ~~said~~ the tender opening sub-system~~,~~ ~~includes~~ performs a decoding operation ~~with~~ using a secret key corresponding to ~~said~~ the public key corresponding to the contract price candidate.

4. (Amended) The electronic tender system as claimed in claim 2, wherein the code processing ~~means~~ section of ~~said~~ the bidder sub-system~~,~~ ~~includes a~~ performs encoding ~~operation of the fixed price by~~ using a public key corresponding to ~~said~~the ~~bidding price~~bid, and

wherein the decoding ~~means~~ section of ~~said~~ the tender opening sub-system~~,~~ ~~includes~~ performs a decoding operation ~~with~~ using a secret key corresponding to ~~said~~ the public key corresponding to the contract price candidate.

5. (Amended) The electronic tender system as claimed in claim 1, wherein said tender opening sub-system includes an announcement ~~means~~ section for announcing one of a portion of a decode parameter acquired ~~in~~ by the decode parameter acquisition ~~means~~ section ~~or~~ and decoding results obtained in the ~~retrieve means~~ determination section for each contract price candidate.

6. (Amended) The electronic tender system as claimed in claim 2, wherein said tender opening sub-system includes an announcement ~~means~~ section for announcing one of a portion of a decode parameter acquired ~~in~~ by the decode parameter acquisition ~~means~~ section ~~or~~ and decoding results obtained in the ~~retrieve means~~ determination section for each contract price candidate.

7. (Amended) The electronic tender system as claimed in claim 3, wherein said tender opening sub-system includes an announcement ~~means~~ section for announcing one of a portion of a decode parameter acquired ~~in~~ by the decode parameter acquisition ~~means~~ section ~~or~~ and decoding results obtained in the ~~retrieve means~~ determination section for each contract price candidate.

8. (Amended) The electronic tender system as claimed in claim 4, wherein said tender opening sub-system includes an announcement ~~means~~ section for announcing one of a portion of a decode parameter acquired ~~in~~ by the decode parameter acquisition ~~means~~ section ~~or~~ and decoding results obtained in the ~~retrieve means~~ determination section for each contract price candidate.

ELECTRONIC TENDER SYSTEM

BACKGROUND OF THE INVENTION

The present invention relates to an electronic tender system, and particularly to a method for coding ~~the bidding price~~a bid and a method for deciding ~~the~~ a contract price.

As known from Japanese Patent Laid-Open No. HEI2-118876, for example, ~~such~~ an electronic tender system ~~adopts a~~ uses coding technology~~,~~ because the ~~bidding price~~bid information should be kept ~~secret generally~~ confidential until the tender opening. ~~The~~ All coded ~~bidding price~~bid information is decoded ~~all at once~~ at the tender opening~~,~~ to decide the highest or the lowest ~~bidding price~~bid ~~among them~~ as the contract price. ~~There,~~ ~~t~~The announcement of all ~~bidding price~~bids allows ~~to everyone~~ all bidders to confirm that the contact price has been decided correctly, in other words, it was the highest or the lowest price among the ~~bidding price~~bids.

Recently, it ~~is demanded~~ has become important not to publish the ~~bidding price~~unaccepted bids ~~not accepted as the contact price, in view of the~~ because of privacy ~~protection~~ concerns. To meet this requirement, for example, an approach has been disclosed in an article, "Multi-round Anonymous Auction Protocols" by Kikuchi, Harkavy and Tyger, published. in "IEEE Workshop on Dependable and Real-time E-Commerce System". This approach disclosed in the prior art literature is shown in Fig. 1.

In this approach, the bidder creates a data row corresponding to ~~his bidding price~~a series indicating bids at successive bid prices. If the bidder wishes to offer a bid at a given price, the bidder's ID is supplied in correspondence to that price. If the bidder does not wish to offer a bid at a given price, a value 0 is supplied in correspondence to that price. This series of data forms a data row. ~~and encodes e~~Each data row is encoded~~respectively~~. The opener receives ~~code string~~ encoded data rows transmitted by all bidders, ~~integrates~~ adds them together and then decodes ~~them~~ the sum to ~~decide~~ determine the contract price. In this approach, as the code string data of individual bidder is not decoded, the ~~bidding price~~bid of respective bidder can be

kept secret, and at the same time, the identification information of the highest price bidder can be extracted from the sum of the data rows~~, by integrating code string data of all bidders~~.

Now, the principle of identification extraction will be described. A bidder having an identification information IDi, creates a data row corresponding to his ~~bidding price~~bids as follows. Suppose the tender reception range be (a, b) and his ~~bidding price~~bid a + v (<b), then (v + 1) times ~~x ID~~ the bidder's ID are concatenated~~enumerated~~. This indicates that the bidder is willing to bid at each corresponding amount. Next, the value 0 ~~are~~ is ~~enumerated~~ concatenated b - (a + v) times. This indicates that the bidder is not willing to bid at any of the corresponding amounts. Thus, a data row containing (b - a + 1) elements is generated.

A data row is then created from each received data row, ~~where~~ in which the respective elements of ~~the~~ each received data row are added~~ by each element is output, by integrating data rows from all bidders generated in this way~~. In ~~this~~ the resulting data row, ~~suppose~~ if the element where 0 appears first ~~be~~ is labeled as the t^{-th}, element, the highest ~~bidding price~~bid (contract price) is the bid corresponding to the a + t -1 element, and the winning bidder ~~who~~ has ~~the~~ identification information in that bidder's data row for the bid corresponding to ~~indicated by the price of~~ the t - 1st element.

However, in this prior art, the ~~bidding~~ bid data becomes longer in proportion to the tender reception price range, because the data row is created in proportion to the length of the tender reception range, and then it is divided to code. Further, when a plurality of bidders have offered the contract price, it is impossible to determine the identification or the number of concerned bidders, because the IDs of the winning bidders have been added together~~decoding result of the t - 1st element is the sum of ID information of bidders of the corresponding bidding price~~.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide an electronic tender system~~, allowing to reduce the bidding~~ that reduces the amount of bid

data, and at the same time, ~~to identify~~ that identifies the ~~concerned~~ winning bidders even when a plurality of bidders have offered the contract price, and moreover, to ~~keep secret the bidding~~ maintain the confidentiality of bid information ~~of~~ for bids other ~~bidding prices~~ than ~~that~~ those of the successful bidders.

Other objects of the present invention will become clear as the description proceeds.

The electronic tender system according to the present invention is characterized ~~by~~ in that a code parameter corresponding to a ~~depending on the bidding price~~bid is delivered to ~~the~~ a coding function section ~~in its~~ of a bidder sub-system. ~~, and, a~~ A contract price candidate selection function selects a candidate price, and a retrieve function ~~by the~~ retrieves a decode parameter ~~depending on~~ corresponding to the candidate price ~~are provided, in order~~ that is used to ~~decide~~ determine whether the candidate contract price is matched in ~~its~~ a tender opening ~~subsystem~~section.

The ~~introduction~~ use of ~~these~~ code parameters and decode parameters that correspond to candidate contract prices allows a bid price to be known ~~realizes an effect to judge~~ only if the ~~bidding price~~bid is identical to ~~the~~ a contract price candidate. Therefore, the highest or the lowest ~~bidding price~~bid and its bidder can be ~~decided,~~ determined by ~~judging if~~ examining in sequence whether there is a ~~bidding price~~bid identical to ~~the~~ a contract price candidate~~, changing~~ and incrementing or decrementing the contract price candidate ~~one by one from the tender~~ with respect to the possible highest price or the lowest price. ~~, and further, how the~~ Bids submitted by other bidders ~~have tendered~~ can be concealed in this manner.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram ~~for~~ showing a conventional method;

Fig. 2 is a block diagram ~~for~~ showing a composition of the present invention; and

Fig. 3 is a block diagram ~~for~~ showing a composition of the retrieve ~~means~~section of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to Figs. 2 and 3, description will proceed to an electronic tender system according to a preferred embodiment of the present invention.

Fig. 2 is a block diagram showing an embodiment of the present invention. The electronic tender system according to the present invention comprises a bidder sub-system 100 and a tender opening sub-system 200. The bidder sub-system 100 includes a code parameter acquisition ~~means~~section 101 and a coding ~~means~~section 102, while the tender opening sub-system 200 includes a reception ~~means~~section 201, a contract price candidate selection ~~means~~section 202, a decode parameter acquisition ~~means~~section 203 and a retrieve ~~means~~section 204.

The retrieve ~~means~~section 204 includes, as shown in Fig. 3, a decoding ~~means~~section 205 and a ~~judgement~~judgment ~~means~~section 206.~~, and the~~ The decoding ~~means~~section 205 sequentially decodes ~~sequentially coded bidding price~~bids received by the reception ~~means~~section 201 ~~based on the~~ using a decode parameter corresponding to a candidate bid that is acquired by the decode parameter acquisition ~~means~~section 205.~~, while the~~ The ~~judgement~~judgment ~~means~~section 206 ~~judges that the coded bidding price~~determines that a decoded bid is identical to the contact price candidate selected by the selection ~~means~~section 202~~, in the case~~ when the decoding result produced by the decoding ~~means~~section 205 ~~becomes a fixed~~ is a predetermined value.

Note that, in this embodiment, to simplify the description, it is supposed, hereinafter, that a bidder subsystem that has offered the highest price, among bid prices, will be decided as the successful bidder, though it is similar in the case where the lowest price will be the successful bid that determines the contract price.

The input to the bidder sub-system 100~~,~~ is the ~~bidding price~~bid desired by ~~this~~ the bidder sub-system. The ~~bidding price~~ bid ~~in~~ by this bidder sub-system 100 is delivered to the code parameter acquisition ~~means~~section 101. In the code parameter acquisition ~~means~~section 101, ~~the~~ a code parameter ~~necessary~~

~~for~~ that is used by the coding ~~means~~section 102 ~~depending on~~ and that corresponds to the amount of this ~~bidding price~~bid is acquired and delivered to the coding ~~means~~section 102. The coding ~~means~~section 102 performs the coding operation based on the supplied code parameter, and delivers the coded bidding data to the transmission ~~means~~section 103. The transmission ~~means~~section 103~~,~~ transmits the coded bidding data to the reception ~~means~~section 201 of the tender opening sub-system 200.

The reception ~~means~~section 201 of the tender opening subsystem 200~~,~~ receives the coded bidding data sent from ~~respective~~ bidder sub-system 100~~,~~ and directs the contract price selection ~~means~~section 202 to ~~start the~~ begin a tender opening process on the tender opening day. The contract price selection ~~means~~section 202 directed to open the tender~~,~~ first~~,~~ takes the highest price within the acceptable range ~~the~~ as a candidate price, and supplie~~d~~s the decode parameter acquisition ~~means~~section 203 with ~~this~~ the candidate price.

The decode parameter acquisition ~~means~~section 203~~,~~ acquires ~~this~~ the decode parameter ~~depending on~~ corresponding to ~~this~~ the candidate price~~,~~ and delivers the decode parameter to the retrieve ~~means~~section 204. The retrieve ~~means~~section 204~~,~~ decodes all coded bidding data received using the supplied decode parameter~~,~~ in the decoding ~~means~~section 205, and the judgment section 206 determines whether ~~retrieves if~~ there is any ~~a bidding price~~bid ~~same as the candidate price~~ among the coded bidding data that is the same as the candidate price~~by the judgement means 206~~. If ~~it is the case~~a matching bid is determined, the ~~bidder~~ bid of the bidder sub-system that ~~has~~ sent ~~that~~ the corresponding coded bidding data will be accepted. If there is no coded bidding data ~~created taking this~~ having the candidate price as its ~~bidding price~~bid, the retrieve ~~means~~section 204~~,~~ outputs that the ~~concerned~~ candidate price is not the contract price to the contract price selection ~~means~~section 202.

Upon the reception of ~~a non candidate signal~~ this output from the retrieve ~~means~~section 204, the contract price selection ~~means~~section 202~~,~~ takes the next lower price than the current candidate price as a new candidate price, and delivers ~~it~~ the new candidate price to the decode parameter acquisition ~~means~~section 203. Then, ~~the similar~~ operations as previously described will be

repeated until the judging ~~means~~section 206 ~~decides~~ detects a successful bidder, or the candidate price becomes lower than the tender ~~possible~~ range. If the candidate price becomes lower than the tender ~~possible~~ range, it is judged that no ~~bidding~~ bid is accepted, and this result is output before terminating the processing.

Now, as an example of this embodiment, the case where an El Gamal code is used as a coding function will be described. ~~The~~ Since the El Gamal code ~~being~~ is well known by those skilled in the art and ~~irrelevant~~ is incidental to the present invention, its detailed explanation will be omitted.

First, the tender opening system creates a large prime p and a generator g. ~~Besides, it decides~~ In addition, a secret key x (v), a public key y (v) and a constant M (v) for a respective ~~bidding price~~bid v are decided. Here, the secret key x (v) and the public key y (v) present the following relation. M (v) may be an arbitrary value, and for example, v and its hash value can be linked as M (v), or ~~it well~~ may be a constant independent of v. As code parameters, M (v) and y (v) are adopted as code parameters and x(v) is adopted as a decode parameter ~~x (v)~~. The code parameters are published, while the decode parameters are ~~severely controlled~~ kept confidential in the tender opening sub-system.

The bidder sub-system 100~~,~~ obtains the code parameters~~,~~ M (v) and y (v)~~,~~ ~~for~~ that correspond to a ~~bidding price~~bid v ~~it desires~~to be made, and codes M (v) with the public key y (v) based on the El Gamal code. The El Gamal code, belonging to the code type called probabilistic encryption, is known to produce a different coded message even if the same M (v) is coded. The bidder sub-system 100~~,~~ sends this coding result to the tender opening system 200 as coded bidding data C (v).

The tender opening sub-system 200 obtains a decode parameter x (v') for a contract price candidate v' and decodes C (v) using this decode parameter as the secret key. ~~There, i~~If v = v' obviously the decoding result will be M(v) = M (v'). On the contrary, if v v', the decoding result will ~~hardly~~ not be M(v'). Thus, without ~~obtaining~~ revealing the ~~bidding price~~bid, it can be ~~judged if it~~ determined whether the bid is equal to the contract price candidate.

If the contract price is decided to be v, all offered code ~~bidding price~~bids, and the decode parameter x (v) corresponding the possible bidding ~~possible~~ prices that are equal to or larger than v are published by the announcement ~~means~~section. Therefore, ~~everyone~~ all bidders can verify that there was no ~~bidding price~~bid larger than v and can determine who has bid the contract price, ~~as~~ since ~~they can try to decode~~ each bidder can attempt to decode all offered code~~d~~ ~~bidding price~~bids using ~~this~~ the announced decode parameter.

On the other hand, ~~bidding price~~bids inferior to the contract price can be concealed, as the decode parameters x (v) corresponding to the ~~bidding price~~bids ~~inferior to~~that are less than the contract price ~~is~~ are not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding subsystems have offered the contract price.

As ~~a~~ another specific embodiment, ~~now~~ a case where RSA code is used for coding function will be described. The detailed description of the RSA code will be omitted as it is well known by those skilled in the art and ~~not relevant~~ is incidental to the present invention. For RSA coding, a code parameter y (v) is generated automatically ~~form~~ from the ~~bidding price~~bid v, without table lookup, and moreover, the fixed value M (v) to be coded may not be fixed for all bidders.

First, the tender opening system generates large primes p and q, and ~~supposes~~ determines ~~n~~ their product n. The bidder sub-system generates ~~as follows~~ the code parameter M (v), y (v), for the ~~bidding price~~bid v it wishes to offer. That ~~it~~ is to say, it generates random numbers, and makes M (v) be the concatenation of v, and this random number, and the hash value where they are coupled. Next, ~~supposing~~ y (v), 1 is concatenated with the hash value of v, making it prime to (p-1)(q-1) ~~each other~~.

Then, M (v) is codified with the public key y (v) based on the RSA code of the modulus n. In this case, as different random numbers are generated for respective bidders, different coded messages are generated even if a same v is coded. The bidder sub-system transmits this coding result to the tender opening system 200 as coded bidding data C (v).

The tender opening system 200 calculates y (v') ~~for~~ corresponding to a contract price candidate v', namely its hash value, and calculates x (v') that is the inverse element of y (v') in the modulus (p- 1)(q-1), as a decode parameter. Then, C (v) is decoded in the modulus n taking this code parameter as the secret key.

Here, if v = v', ~~obviously,~~ the decoding result M (v') will ~~be~~ have a correct format ~~by~~ for v' and a certain random number. On the other hand, if v v', the decoding result will ~~hardly be~~ not have such format. Thus, without ~~obtaining~~ revealing the ~~bidding price~~bid ~~it self~~itself, it can be ~~judged if it~~ determined whether the bid is equal to the contract price candidate.

If the contract price is decided to be v, all offered code ~~bidding price~~bids, and respective result of decoding by the decode parameter x (v) corresponding the possible tender ~~possible~~ prices that are equal to or larger than v are published by the announcement ~~means~~section. Therefore, ~~everyone~~ all bidders can verify that there was no ~~bidding price~~bid larger than v and identify the successful bidder~~who has bid the contract price~~, ~~as~~ since they can confirm that the result coded by the code parameter y (v') corresponding to the contact price candidate is equal to the offered ~~respective~~ coded ~~bidding price~~bids~~,~~ using ~~this~~ the announced decode parameter.

On the other hand, ~~bidding price~~bids inferior to the contract price can be concealed, ~~as~~ because the decoding result corresponding to the ~~bidding price~~bids that are less than ~~inferior to~~ the contract price ~~is~~ are not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding subsystems have offered the contract price.

Moreover, it is assured that coded ~~bidding price~~bids to be input into the tender opening system excludes those outside the bidding period, by publishing coded ~~bidding price~~bids that are received before the bidding deadline, and opening only ~~those~~ the published bids~~ones~~. As ~~it is irrelevant~~ this is incidental to the present invention, ~~the~~ further detailed description ~~thereof~~ of this feature will be omitted.

Additionally, it can be assured that the tender opening system will not ~~decode~~ illegally decode the coded ~~bidding price~~bid, such as by controlling or generating ~~the~~ different decode parameters ~~with~~ using a plurality of sub-systems~~,~~ that employ a ~~using~~ distributed secret or group decryption technology or the like. As ~~it is also irrelevant~~ this feature is also incidental to the present invention, ~~the~~ further detailed description ~~thereof~~ will be omitted.

~~Beside~~ In addition, a digital signature ~~of the~~ may be used with a coded ~~bidding price~~bid ~~can be added,~~ in order to prevent the bidder from bidding in the name of ~~the other~~another bidder, or denying ~~later the~~ responsibility for a transmitted coded ~~bidding price~~bid; however, ~~as it is also irrelevant~~ this feature is also incidental to the present invention, ~~the~~ so further detailed description thereof will be omitted.

In ~~this~~ the disclosed embodiment, ~~to simplify,~~ the case where a bidding sub-system that has offered the highest price~~,~~ among bid prices~~, will be decided~~ ~~as~~ is the successful bidder has been described in detail; however, similarly, ~~it can easily~~ the invention may also be applied to the case wherein the lowest price will be the contract price, or to the case wherein a plurality of bidding sub-systems that have offered a ~~bidding price~~bid close to the highest price or the lowest price are treated as winning bidders.

It is to be understood that the present invention is not limited to the aforementioned respective embodiments, and obviously, the respective embodiments can be executed by conveniently modifying them, without departing from the technical concept of the present invention.

As described hereinbefore, according to the present invention, it is possible to provide an electronic tender system~~, allowing to~~ that selects the bidder who has offered the highest or the lowest price as successful bidder, and moreover, ~~to keep secret the~~ that maintains the confidentiality of bidding information ~~of~~ for ~~other bidding price~~bids other than ~~that~~ those of the successful bidders, based on a basic composition wherein ~~the~~ bidder sub-systems ~~codes~~ code their bids by means of a code parameter ~~depending on the bidding price~~that corresponds to a particular bid value, and the tender opening system

decodes by a decode parameter ~~depending on the~~ that corresponds to a particular contract price candidate.

ABSTRACT

~~The~~ A coding function section in ~~the~~ a bidder sub-system ~~100~~ is supplied~~,~~ with a code parameter ~~depending on the bidding price~~that corresponds to a bid to be offered, and the ~~bidding price~~bid is coded ~~depending on this~~ using the code parameter. ~~The~~ A tender opening system ~~200~~ decodes received bids ~~sequentially the~~ using a decode parameter corresponding to ~~the highest bidding price starting from the~~ a highest or ~~the~~ lowest ~~one among bidding prices that can possibly be accepted~~bid amount in a predetermined bid range, and ~~the one~~ any bid that is successfully decoded using the decode parameter is ~~judged to be a bidding price corresponding to that parameter and~~ accepted as the contract price. If no bid is decoded using the decode parameter of the highest/lowest amount of the range, the tender opening system attempts to decode all bids using the decode parameter of the next highest/lowest bid in the range. ~~The~~ In this manner information ~~of~~ regarding unaccepted ~~bidding price~~bids ~~will be concealed~~is kept confidential~~,~~ by not publishing the decode parameters concerning the ~~bidding price~~bids ~~of the order~~ inferior to the ~~contract price~~winning bid.